The groups of points on abelian surfaces over finite fields

Sergey Rybakov

Abstract. Let A be an abelian surface over a finite field k. The k-isogeny class of A is uniquely determined by a Weil polynomial f_A of degree 4. We give a classification of the groups of k-rational points on varieties from this class in terms of f_A.

1. Introduction

Classical results of Tate and Honda give us an explicit description for the set of isogeny classes of abelian varieties over a finite field k. Namely, an isogeny class is uniquely determined by a so called Weil polynomial of any variety from this class. It looks natural to consider classification problems concerning abelian varieties inside a given isogeny class. In this paper we classify groups of k-rational points on abelian surfaces. Xing partly classified groups of points on supersingular surfaces in [**Xi94**] and in [**Xi96**]. In the paper [**Ry10**] we show that one could use the language of Hodge polygons to describe groups of points. Moreover, we classify this groups for abelian varieties with commutative endomorphism algebra. An abelian variety has commutative endomorphism algebra if and only if its Weil polynomial has no multiple roots. We could say that this is the general case. From the classification of Weil polynomials of abelian surfaces due to Rück, Xing, Maisner and Nart [**MN02**] we get that there are only three cases more. Namely,

- the Weil polynomial is a square of a polynomial of degree 2 without multiple roots;
- the Weil polynomial is of the form $P(t)(t \pm \sqrt{q})^2$, where $P(t)$ has no multiple roots, and $\sqrt{q} \in \mathbb{Z}$;
- the Weil polynomial equals $(t \pm \sqrt{q})^4$, and $\sqrt{q} \in \mathbb{Z}$.

The paper is devoted to a classification of groups of points for these three cases.

The author is grateful to referee for providing useful corrections on the paper.

1991 *Mathematics Subject Classification.* 14K99, 14G05, 14G15.

Key words and phrases. abelian variety, the group of rational points, finite field, Newton polygon, Hodge polygon.

Supported in part by RFBR grants no. 11-01-00393-a, 11-01-12072-ofi-m and 10-01-93110-CNRSLa.

2. Main result

Throughout this paper k is a finite field $\mathbb{F}_q$ of characteristic p. Let A be an abelian variety of dimension g over k, and let $\bar{k}$ be an algebraic closure of k. Fix a prime number ℓ. For a natural number m denote by A_m the kernel of multiplication by ℓ^m in $A(\bar{k})$. Let $T_\ell(A) = \varprojlim A_m$ be the Tate module, and $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ be the corresponding vector space over $\mathbb{Q}_\ell$. If $\ell \neq p$, then $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. The Frobenius endomorphism F of A acts on the Tate module by a semisimple linear operator, which we also denote by $F : T_\ell(A) \to T_\ell(A)$. The characteristic polynomial

$$f_A(t) = \det(t - F | T_\ell(A))$$

is called a *Weil polynomial of* A. It is a monic polynomial of degree $2g$ with rational integer coefficients independent of the choice of prime $\ell \neq p$. It is well known that for isogenous varieties A and B we have $f_A(t) = f_B(t)$. Moreover, Tate proved that the isogeny class of abelian variety is determined by its characteristic polynomial, that is $f_A(t) = f_B(t)$ implies that A is isogenous to B (see [**WM69**]). If $\ell = p$, then $T_p(A)$ is called a *physical Tate module*. In this case, $f_A(t) = f_1(t) f_2(t)$, where $f_1, f_2 \in \mathbb{Z}_p[t]$, and $f_1(t) = \det(t - F | T_p(A))$. Moreover $d = \deg f_1 \leq g$, and $f_2(t) \equiv t^{2g-d} \mod p$ (see [**De78**]).

Recall some definitions and results from [**Ry10**]. For an abelian group G we denote by G_ℓ the ℓ-primary component of G. The group $A(k)$ is a kernel of $1 - F : A \to A$, and the ℓ-component

$$A(k)_\ell \cong T_\ell(A)/(1 - F)T_\ell(A)$$

(see [**Ry10**, Proposition 3.1]). The proof of the following lemma is essentially the proof of [**Ry10**, Theorem 1.1].

LEMMA 2.1. *Let A be an abelian variety over k, and let G be a finite abelian group of order $f_A(1)$. Suppose that for any prime number ℓ dividing order of G we have an F-invariant sublattice $T_\ell \subset T_\ell(A)$ such that $G_\ell \cong T_\ell/(1 - F)T_\ell$. Then there exists an abelian variety B over k, and an isogeny $\varphi : B \to A$ such that $T_\ell(\varphi)$ induces an isomorphism $T_\ell(B) \cong T_\ell$ for any ℓ. In particular, $B(k) \cong G$.*

We need a modification of this statement. Suppose we are looking for an abelian variety B such that $B(k) \cong G$, and A and B are isogenous. It is enough to find free $\mathbb{Z}_\ell$ module T_ℓ for any ℓ with semisimple action $F : T_\ell \to T_\ell$ such that $f_A(t) = \det(t - F)$, and $G_\ell \cong T_\ell/(1 - F)T_\ell$. Indeed, since the Frobenius action on the vector space V_ℓ is semisimple, it is determined up to isomorphism by the Weil polynomial f_A. We can reconstruct this action as follows. Put $V'_\ell = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, and choose any inclusion $T_\ell(A) \to V'_\ell$ such that the image of $T_\ell(A)$ contains T_ℓ. Clearly, this inclusion induces an isomorphism of F-vector spaces $V_\ell \to V'_\ell$.

Let $Q(t) = \sum_i Q_i t^i$ be a polynomial of degree d over $\mathbb{Q}_\ell$, and let $Q(0) = Q_0 \neq 0$. Take the lower convex hull of the points $(i, \mathrm{ord}_\ell(Q_i))$ for $0 \leq i \leq d$ in $\mathbb{R}^2$. The boundary of this region without vertical lines is called *the Newton polygon* $\mathrm{Np}_\ell(Q)$ *of* Q. Its vertices have integer coefficients, and $(0, \mathrm{ord}_\ell(Q_0))$ and $(d, \mathrm{ord}_\ell(Q_d))$ are its endpoints. One can associate to $\mathrm{Np}(Q)$ the set of its slopes, and each slope has a multiplicity. The Newton polygon of Q is uniquely determined by this data. Suppose we have two polynomials Q_1 and Q_2. Then the slope set for $\mathrm{Np}(Q_1 Q_2)$

is the union of slope sets for $\mathrm{Np}(Q_1)$ and $\mathrm{Np}(Q_2)$, and multiplicities of slopes of $\mathrm{Np}(Q_1Q_2)$ are sums of multiplicities of corresponding slopes of $\mathrm{Np}(Q_1)$ and $\mathrm{Np}(Q_2)$.

We associate to $A(k)_\ell$ a polygon of special type.

DEFINITION 2.2. Let $0 \le m_1 \le m_2 \le \cdots \le m_r$ be nonnegative integers, and let $H = \oplus_{i=1}^r \mathbb{Z}/\ell^{m_i}\mathbb{Z}$ be an abelian group of order ℓ^m. The *Hodge polygon* $\mathrm{Hp}_\ell(H, r)$ *of a group* H is the convex polygon with vertices $(i, \sum_{j=1}^{r-i} m_j)$ for $0 \le i \le r$. It has $(0, m)$ and $(r, 0)$ as its endpoints, and its slopes are $-m_r, \ldots, -m_1$. We write $\mathrm{Hp}(H) = (m_1, \ldots, m_r)$.

Note that some of the numbers m_i could be zero, in other words, the Hodge polygon is allowed to have zero slopes. The isomorphism class of H depends only on $\mathrm{Hp}_\ell(H, r)$. When we work with groups of points on abelian surfaces we often write $\mathrm{Hp}_\ell(H) = \mathrm{Hp}_\ell(H, 4)$. We need the following well-known result (see [**Ke10**, 4.3.8] or [**BO**, 8.40]).

THEOREM 2.3. *Let E be an injective endomorphism of a free $\mathbb{Z}_\ell$-module T of finite rank. Let $f(t) = \det(E - t)$ be its characteristic polynomial. Then $\mathrm{Np}_\ell(f)$ lies on or above the Hodge polygon of T/ET, and these polygons have same endpoints.*

Weil polynomials of abelian surfaces were classified by Rück, Xing, Maisner and Nart [**MN02**]. We use a simplified version of this classification. Namely, we use that for the Weil polynomial only four cases of the main theorem below occur.

THEOREM 2.4. *Let A be an abelian surface over a finite field with Weil polynomial f_A. Let G be an abelian group of order $f_A(1)$. Then G is a group of points on some variety in the isogeny class of A if and only if for any prime number ℓ*

1. *if f_A has no multiple roots, then $\mathrm{Np}_\ell(f_A(1-t))$ lies on or above $\mathrm{Hp}_\ell(G_\ell)$;*
2. *if $f_A = P_A^2$, and P_A has no multiple roots, then $G_\ell \cong G_\ell^{(1)} \oplus G_\ell^{(2)}$, where $G_\ell^{(1)}$ and $G_\ell^{(2)}$ are ℓ-primary abelian groups with one or two generators such that $\mathrm{Np}_\ell(P_A(1-t))$ lies on or above $\mathrm{Hp}_\ell(G_\ell^{(1)}, 2)$ and $\mathrm{Hp}_\ell(G_\ell^{(2)}, 2)$.*
3. *Suppose $f_A = (t^2 - bt + q)(t \pm \sqrt{q})^2$, and $\sqrt{q} \in \mathbb{Z}$, where $f(t) = t^2 - bt + q$ has no multiple roots; let*
   - *$\mathrm{Hp}_\ell(G_\ell) = (m_1, m_2, m_3, m_4)$;*
   - *$m = \mathrm{ord}_\ell(f(1))$;*
   - *$m_q = \mathrm{ord}_\ell(1 \pm \sqrt{q})$;*
   - *$m_b = m_1 + m_3 - m_q$.*

   Then
   (a) $0 \le m_b \le \mathrm{ord}_\ell(b-2)$;
   (b) $\min(m_b, m_q) \ge m_1$;
   (c) $\min(m - m_b, m_q) \ge m_2$.
4. *Finally, if $f_A(t) = (t \pm \sqrt{q})^4$, and $\sqrt{q} \in \mathbb{Z}$, then $G \cong (\mathbb{Z}/(1 \pm \sqrt{q})\mathbb{Z})^4$.*

PROOF. Case (1) follows from [**Ry10**]. Let us prove that conditions of the case (2) are necessary. First, suppose that a prime ℓ divides $f_A(1)$, but $P_A(1-t) \not\equiv t^2 \bmod \ell$. It is equivalent to say that $P_A(1-t) = (t - x_1)(t - x_2)$, where $x_1, x_2 \in \mathbb{Z}_\ell$, and ℓ divides x_1, but not divides x_2. Thus $T_\ell(A)$ is a direct sum of two modules T_1 and T_2 of $\mathbb{Z}_\ell$-rank two such that $1 - F$ acts on T_i as multiplication by x_i. It follows that

$$G_\ell \cong T_1/(1-F)T_1 \cong (\mathbb{Z}_\ell/x_1\mathbb{Z}_\ell)^2,$$

and $G_\ell^{(1)} \cong G_\ell^{(2)} \cong \mathbb{Z}_\ell/x_1\mathbb{Z}_\ell$. The rest follows from Theorem 3.4 below. To prove that the conditions of (2) are sufficient we have to find an abelian variety B with a given group of points G. By Lemma 2.1 it is enough to construct a Tate module $T_\ell(B)$ for any prime ℓ dividing $f_A(1)$. By [**Ry10**, Theorem 3.2] there exist F-invariant $\mathbb{Z}_\ell$-modules T_1' and T_2' such that $T_i'/(1-F)T_i' \cong G_\ell^{(i)}$, and $T_i' \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell[t]/P_A(t)\mathbb{Q}_\ell[t]$ for $i \in \{1,2\}$. Now we let $T_\ell(B) \cong T_1' \oplus T_2'$.

We prove the case (3) in the last section. The case (4) is obvious since F acts as multiplication by $\mp\sqrt{q}$. □

3. Matrix factorizations

In this section we finish the proof of case (2). We assume that ℓ divides $P_A(1)$ and that

$$P_A(1-t) \equiv t^2 \mod \ell.$$

In this case $\ell \neq p$. Indeed, let $P_A(t) = t^2 - bt + c$, where $c = \pm q$. If $\ell = p$ satisfies our assumptions, we get that $2-b$ and $1-b$ are both divisible by p.

In [**Ry**] we show that the Tate module $T_\ell(A)$ corresponds to a matrix factorization. Fix a pair of polynomials $f, f_1 \in \mathbb{Z}_\ell[t]$ and a positive integer r. Put $R = \mathbb{Z}_\ell[t]/f_1\mathbb{Z}_\ell[t]$. Denote by $x \in R$ the image of t under the natural projection from $\mathbb{Z}_\ell[t]$.

Definition 3.1. A matrix factorization (X, Y) is a pair of $r \times r$ matrices with coefficients in $\mathbb{Z}_\ell[t]$ such that $\det X = f$ and $YX = f_1 \cdot I_r$, where I_r is the identity matrix.

Suppose we are given a matrix factorization (X, Y). The matrix X defines a map of free $\mathbb{Z}_\ell[t]$ modules:

$$\mathbb{Z}_\ell[t]^r \xrightarrow{X} \mathbb{Z}_\ell[t]^r.$$

Its cokernel T is annihilated by f_1. It is equivalent to say that T is an R-module. We see that the matrix factorization (X, Y) corresponds to a finitely generated R-module T given by the presentation:

$$\mathbb{Z}_\ell[t]^r \xrightarrow{X} \mathbb{Z}_\ell[t]^r \to T \to 0. \tag{3.1}$$

Proposition 3.2. [**Ry**, Proposition 5.2] *Suppose* $f_1 \equiv t^{d_1} \mod \ell$, *and* $\deg f_1 = d_1$. *The module* T *is free of finite rank over* $\mathbb{Z}_\ell$, *and characteristic polynomial of the action of* x *on* T *is equal to* f.

The following proposition shows that modules over R give rise to matrix factorizations.

Proposition 3.3. *Let* T *be an* R*-module which is free of finite rank over* $\mathbb{Z}_\ell$. *Suppose that* T *can be generated over* R *by* r *elements, and that* $\mathrm{Hp}(T/xT) = (m_1, \ldots, m_r)$. *Then there exists a matrix factorization* (X, Y) *such that* T *has presentation* (3.1), *and*

$$X \equiv \mathrm{diag}(\ell^{m_1}, \ldots, \ell^{m_r}) \mod t\mathbb{Z}_\ell[t].$$

Proof. By [**Ry**, Proposition 5.3] there exists a matrix factorization (X_1, Y_1) such that T has presentation

$$\mathbb{Z}_\ell[t]^r \xrightarrow{X_1} \mathbb{Z}_\ell[t]^r \to T \to 0. \tag{3.2}$$

Take the cokernel of the multiplication by t of the presentation(3.2); we get

$$\mathbb{Z}_\ell^r \xrightarrow{\bar{X}_1} \mathbb{Z}_\ell^r \to T/xT \to 0.$$

There exist matrices M_1 and M_2 over $\mathbb{Z}_\ell$ such that $\det M_1 = \det M_2 = 1$ and $\bar{X} = M_1 \bar{X}_1 M_2$ is a diagonal matrix. Since

$$\mathbb{Z}_\ell^r/\bar{X}\mathbb{Z}_\ell^r \cong T/xT,$$

we get that $\bar{X} = \operatorname{diag}(\ell^{m_1}, \dots, \ell^{m_r})$. Now take $X = M_1 X_1 M_2$ and $Y = M_2^{-1} Y_1 M_1^{-1}$. □

THEOREM 3.4. *Assume that $f_A = P_A^2$, and $P_A(1-t) \equiv t^2 \mod \ell$. Suppose that P_A has no multiple roots. Then $A(k)_\ell \cong G_\ell^{(1)} \oplus G_\ell^{(2)}$, where $G_\ell^{(1)}$ and $G_\ell^{(2)}$ are ℓ-primary abelian groups with one or two generators such that $\operatorname{Np}_\ell(P_A(1-t))$ lies on or above $\operatorname{Hp}_\ell(G_\ell^{(1)}, 2)$ and $\operatorname{Hp}_\ell(G_\ell^{(2)}, 2)$.*

PROOF. Apply Theorem 2.3 to $T = T_\ell(A)$ and $E = 1 - F$. The slopes of $\operatorname{Np}(P_A(1-t))$ are the slopes of $\operatorname{Np}(P_A(1-t)^2)$, but multiplicities are doubled. We get that m_1 is not greater than the smallest slope of $\operatorname{Np}(P_A(1-t))$, i.e. that ℓ^{m_1} divides $b-2$. It is enough to prove that $m := \operatorname{ord}_\ell(P_A(1)) = m_1 + m_4$. Indeed, in this case $\operatorname{Np}_\ell(P_A(1-t))$ lies on or above $\operatorname{Hp}_\ell(G_\ell^{(1)}, 2) = (m_1, m_4)$. Moreover, $m = m_2 + m_3$, and by Lemma 3.5 below $\operatorname{Np}_\ell(P_A(1-t))$ lies on or above $\operatorname{Hp}_\ell(G_\ell^{(2)}, 2) = (m_2, m_3)$.

Note that m_4 is a minimal number such that $\frac{\ell^{m_4}}{F-1} \in \operatorname{End} A$, and m_1 is a maximal number such that ℓ^{m_1} divides $F-1$. From the equality $(F-1)^2 - (b-2)(F-1) - P_A(1) = 0$ we get that

$$\frac{P_A(1)}{(F-1)\ell^{m_1}} = \frac{F-1}{\ell^{m_1}} - \frac{b-2}{\ell^{m_1}} \in \operatorname{End} A.$$

It follows that $m \geq m_1 + m_4$.

The Frobenius action on the Tate module $T_\ell(A)$ is determined up to isomorphism by a module structure over the ring $R = \mathbb{Z}_\ell[t]/P_A(1-t)\mathbb{Z}_\ell[t]$ with t acting as $1 - F$. Suppose we have an R-module T such that $\operatorname{Hp}(T/xT) = (m_1, m_2, m_3, m_4)$. By Proposition 3.3 there exists a matrix factorization (X, Y) such that $\det X = f_A(1-t)$ and

$$X \equiv \operatorname{diag}(\ell^{m_1}, \ell^{m_2}, \ell^{m_3}, \ell^{m_4}) \mod t\mathbb{Z}_\ell[t].$$

The matrix factorization (Y, X) corresponds to a module T' over R, which is generated by 4 elements and the characteristic polynomial of x is equal to $\det Y = P_A^4(1-t)/f_A(1-t) = f_A(1-t)$. Moreover,

$$Y \equiv \operatorname{diag}(\ell^{m-m_1}, \ell^{m-m_2}, \ell^{m-m_3}, \ell^{m-m_4}) \mod t\mathbb{Z}_\ell[t],$$

i.e. $\operatorname{Hp}(T'/xT') = (m-m_1, m-m_2, m-m_3, m-m_4)$. By Lemma 2.1 there exists an abelian surface B such that $T_\ell(B) \cong T'$. From the first part of the proof applied to $T_\ell(B)$ it follows that $(m-m_1) + (m-m_4) \leq m$. Thus $m = m_1 + m_4$. □

LEMMA 3.5. $m_2 \leq \operatorname{ord}_\ell(b-2)$.

PROOF. Let L be a splitting field of P_A over $\mathbb{Q}_\ell$, and let S be its ring of integers. We have $P_A(1-t) = (t-a)(t-c)$, where $a, c \in S$, and $\operatorname{ord}_\ell(a) \leq \operatorname{ord}_\ell(b-2)$. (Here $\operatorname{ord}_\ell(a) \in \frac{1}{2}\mathbb{Z}$.) Consider the map

$$E = F + a - 1 : T_\ell(A) \otimes_{\mathbb{Z}_\ell} S \to T_\ell(A) \otimes_{\mathbb{Z}_\ell} S.$$

Then $1-F$ acts on $T_1 = \ker E$ as multiplication by a. We get an exact sequence:

$$0 \to T_1 \to T_\ell(A) \otimes_{\mathbb{Z}_\ell} S \to T_2 = \operatorname{Im} E \to 0,$$

where $\operatorname{rk}_S T_1 = \operatorname{rk}_S T_2 = 2$. Act by $1-F$ on this sequence. By snake lemma we get an exact triple of abelian groups:

$$0 \to (S/aS)^2 \to A(k)_\ell \otimes_{\mathbb{Z}_\ell} S \to G' \to 0.$$

If $S = \mathbb{Z}_\ell$ then $A(k)_\ell$ contains $(\mathbb{Z}_\ell/a\mathbb{Z}_\ell)^2$, and $G' = T_2/(1-F)T_2$ is generated by 2 elements. It follows that $m_2 \le \operatorname{ord}_\ell(a)$. If $S \ne \mathbb{Z}_\ell$, then $S \cong \mathbb{Z}_\ell^2$ as $\mathbb{Z}_\ell$-module and we multiply everything by two: $A(k)_\ell^2$ contains

$$(S/aS)^2 \cong (\mathbb{Z}/\lfloor \operatorname{ord}_\ell(a) \rfloor \mathbb{Z})^2 \oplus (\mathbb{Z}/\lceil \operatorname{ord}_\ell(a) \rceil \mathbb{Z})^2,$$

and $G' = T_2/(1-F)T_2$ is generated by 4 elements. Thus $m_2 \le \lfloor \operatorname{ord}_\ell(a) \rfloor \le \operatorname{ord}_\ell(b-2)$. □

4. Proof of case 3

The conditions (b) and (c) are equivalent to the following inequalities:

(1) $m_1 \le m_b$, which is equivalent to $m_3 \ge m_q$;
(2) $m_1 \le m_q$;
(3) $m_2 \le m_q$;
(4) $m_2 \le m - m_b$, which is equivalent to $m_4 \ge m_q$, since $f_A(1) = m_1 + m_2 + m_3 + m_4 = m + 2m_q$.

Note that inequalities $m_b \ge 0$ and (4) follow from (1), and (2) follows from (3). We have to prove (3), (1) and the second part of (a).

Let $\alpha = 1 \pm \sqrt{q}$, and let $G_\ell = A(k)_\ell$. Consider the map $E = F + \alpha - 1 : T_\ell(A) \to T_\ell(A)$. Then $1-F$ acts on $T_1 = \ker E$ by multiplication by α, and $1-F$ acts on $T_2 = \operatorname{Im} E$ with characteristic polynomial $f(1-t)$. We get an exact sequence:

$$0 \to T_1 \to T_\ell(A) \to T_2 \to 0,$$

and by the snake lemma

$$0 \to (\mathbb{Z}/\ell^{m_q}\mathbb{Z})^2 \to G_\ell \to G' \to 0.$$

The group G_ℓ contains $(\mathbb{Z}/\ell^{m_q}\mathbb{Z})^2$ only if $m_3 \ge m_q$, and G' has two generators only if (3) holds.

We now prove (a). Since $\operatorname{Hp}_\ell(T_\ell(A)/(F-1)T_\ell(A)) = (m_1, m_2, m_3, m_4)$ there exists a basis $v_1, v_2, v_3, v_4 \in T_\ell(A)$ such that

$$(F-1)v_1 \in \ell^{m_1} T_\ell(A),\ (F-1)v_2 \in \ell^{m_2} T_\ell(A),$$

$$(F-1)v_3 \in \ell^{m_3} T_\ell(A), \text{ and } (F-1)v_4 \in \ell^{m_4} T_\ell(A). \qquad (*)$$

The vectors Ev_4 and Ev_3 generate a lattice $T_3 \subset T_2$ of rank 2, thus $1-F$ acts on T_3 with characteristic polynomial $f(1-t)$. By Theorem 2.3 the Newton polygon $\operatorname{Np}_\ell(f(1-t))$ lies on or above $\operatorname{Hp}(T_3/(F-1)T_3, 2)$. Thus, we can find a linear combination v_3' of v_4 and v_3 such that v_1, v_2, v_3', v_4 is a basis and $(*)$ holds, but $(F-1)Ev_3'$ is not divisible by $(b-2)\ell$ in T_3. On the other hand, $F - 1 = E - \alpha$, and since $m_3 \ge m_q$, it follows that Ev_3' is not divisible by $\alpha\ell$ in $T_\ell(A)$. We proved that $(F-1)Ev_3'$ is not divisible by $\alpha(b-2)\ell$ in $T_\ell(A)$. By definition, $(F-1)v_3'$ is divisible by ℓ^{m_3} in $T_\ell(A)$. By the first inequality, $m_q \ge m_1$; thus for any vector

$v \in T_\ell(A)$ the vector Ev is divisible by ℓ^{m_1} in $T_\ell(A)$. We finally get that $(F-1)Ev_3'$ is divisible by $\ell^{m_1+m_3}$, but not divisible by $\ell\alpha(b-2)$ in $T_\ell(A)$. Thus

$$m_1 + m_3 < m_q + \mathrm{ord}_\ell(2-b) + 1.$$

Let us construct an abelian variety with a given group of points. We give an explicit construction of the Tate module T_ℓ such that $T_\ell/(F-1)T_\ell \cong G_\ell$, and apply Lemma 2.1. By assumption, we have an isomorphism of F-vector spaces:

$$V_\ell(A) \cong \mathbb{Q}_\ell[t]/P_A(1-t) \oplus (\mathbb{Q}_\ell[t]/(\alpha - t))^2,$$

where t acts as $1-F$ on the right-hand side. Thus there exists a basis v_1, v_2, v_3, v_4 of $V_\ell(A)$ such that

$$(1-F)v_1 = \ell^{m_b}v_2 + (b-2)v_1, \quad (1-F)v_2 = -\ell^{-m_b}f(1)v_1,$$
$$(1-F)v_3 = \alpha v_3, \qquad (1-F)v_4 = \alpha v_4.$$

Let T_ℓ be the $\mathbb{Z}_\ell$-submodule of $V_\ell(A)$ generated by

$$u_1 = v_1 + v_3, \qquad u_3 = v_2 + v_4,$$
$$u_2 = \frac{(1-F)u_1 - (b-2+\alpha)u_1 - \ell^{m_b}u_3}{\ell^{m_1}}, \text{ and}$$
$$u_4 = \frac{(1-F)u_3 - \alpha u_3 + \frac{f(1)}{\ell^{m_b}}u_1}{\ell^{m_2}}.$$

A straightforward calculation shows that

$$(1-F)u_1 = \ell^{m_1}u_2 + (b-2+\alpha)u_1 + \ell^{m_b}u_3;$$
$$(1-F)u_3 = \ell^{m_2}u_4 + \alpha u_3 - \frac{f(1)}{\ell^{m_b}}u_1;$$
$$(1-F)u_2 = \frac{-(b-2)\alpha u_1 - \ell^{m_b}\alpha u_3}{\ell^{m_1}};$$
$$(1-F)u_4 = \frac{f(1)\alpha u_1}{\ell^{m_2+m_b}} \in \ell^{m_4}T_\ell.$$

By (a) and (1), the vector $(1-F)u_1 \in \ell^{m_1}T_\ell$; by (3) and (4), the vector $(1-F)u_3 \in \ell^{m_2}T_\ell$; by (a) the vector $(1-F)u_2 \in \ell^{m_3}T_\ell$; by definition of m_b, the vector $(1-F)u_4 \in \ell^{m_4}T_\ell$. We get that the natural surjective map $T_\ell \to G_\ell$ factors through a surjective map $T_\ell/(1-F)T_\ell \to G_\ell$. We conclude that $T_\ell/(1-F)T_\ell \cong G_\ell$, since orders of both groups coincide.

References

[BO] Berthelot P., Ogus A., Notes on crystalline cohomology, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1978.

[De78] Demazure M., Lectures on p-divisible groups, Lecture notes in mathematics 302, Springer-Verlag, Berlin, 1972.

[Ke10] Kedlaya K., p-adic differential equations, Cambridge University Press, 2010.

[MN02] D. Maisner, E. Nart. *Abelian surfaces over finite fields as Jacobians.* With an appendix by Everett W. Howe. Experiment. Math. 11 (2002), no. 3, 321–337.

[Ry10] S. Rybakov. *The groups of points on abelian varieties over finite fields.* Cent. Eur. J. Math. 8(2), 2010, 282-288. arXiv:0903.0106v4

[Ry] S. Rybakov. *The finite group subschemes of abelian varieties over finite fields.* arXiv:1006.5959v1

[Wa69] Waterhouse W., Abelian varieties over finite fields, Ann. scient. Éc. Norm. Sup., 1969, 4 serie 2, 521–560.

[WM69] Waterhouse W., Milne J., Abelian varieties over finite fields, Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969, 53–64.

[Xi94] Xing Ch., The structure of the rational point groups of simple abelian varieties of dimension two over finite fields, Arch. Math., 1994,63, 427–430.

[Xi96] Xing Ch., On supersingular abelian varieties of dimension two over finite fields, Finite Fields Appl., 1996, 2, no. 4, 407–421.

Poncelet laboratory (UMI 2615 of CNRS and Independent University of Moscow)

Institute for information transmission problems of the Russian Academy of Sciences

Laboratory of Algebraic Geometry, GU-HSE, 7 Vavilova Str., Moscow, Russia, 117312

E-mail address: rybakov@mccme.ru, rybakov.sergey@gmail.com